05-08-06

AF

JFW

Attorney Docket No.: PALM-3217.SG

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

I hereby certify that this transmittal of the below described documents is being deposited with the United States Postal Service in an envelope bearing Express Mail Postage and an Express Mail label, with the below serial number, addressed to the Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450, on the below date of deposit.			
Express Mail Label No.:	EV757242723US	Name of Person Making the Deposit:	Jose S. Garcia
Date of Deposit:	5/5/2006	Signature of the Person Making the Deposit:	Jose S. Garcia

In re Application of: Steve Lemke

Application Serial No. : 09/769,654 Group Art Unit: 2137

Filed : 01/24/2001 Examiner: FIELDS, C.

For : HANDHELD COMPUTER SYSTEM CONFIGURED TO AUTHENTICATE A USER AND POWER-UP IN RESPONSE TO A SINGLE ACTION BY THE USER

Commissioner for Patents
P.O Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF TRANSMITTAL

1. Transmitted herewith is an Appeal Brief for this application

X Transmitted herewith is an Appeal Brief for the above identified patent application.
(26 sheets)

2. Applicant is other than a small entity

Extension of Term

3. The proceedings herein are for a patent application and the provisions of 37 C.F.R. 1.136 apply.

(a) [ ] Applicant petitions for an extension of time under 37 C.F.R. 1.136
(fees: 37 C.F.R. 1.17(a)-(d) for the total number of months checked below:)

Extension	Fee
[ ] one month	$120.00
[ ] two months	$450.00
[ ] three months	$1,020.00
[ ] four months	$1,590.00

Fee $ 0.00

If an additional extension of time is required, please consider this a petition therefor.

(b) [X]Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition for extension of time.

4. Fee Payment ($500.00)

The fee required is paid as follows:

[X] The Commissioner is hereby authorized to charge any fees associated with this communication or credit any overpayment to Deposit Account No.: 23-0085.
A duplicate copy of this authorization is enclosed.

[ ] A check in the amount of _____

[ ] Charge any fees required or credit any overpayments associated with this filing to Deposit Account No.: 23-0085.

Please direct all correspondence concerning the above-identified application to the following address:

WAGNER, MURABITO & HAO LLP
Two North Market Street, Third Floor
San Jose, California 95113
(408) 938-9060

Respectfully submitted,

Date: 5/5/2006

By: Jose S. Garcia
Jose S. Garcia
Reg. No. 43,628

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Steve Lemke

Application Serial No.: 09/769,654 Group Art Unit: 2137

Filed : 01/24/2001 Examiner: FIELDS, C.

For : HANDHELD COMPUTER SYSTEM CONFIGURED TO AUTHENTICATE A USER AND POWER-UP IN RESPONSE TO A SINGLE ACTION BY THE USER

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

A Final Office Action was mailed 11/03/2005. In response, a Notice of Appeal was submitted, which the USPTO indicated the date of receipt as being March 6, 2006. Thus, the Appeal Brief is due on May 6, 2006, which is two months from March 6, 2006, the date of receipt of the Notice of Appeal.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party in interest is PALM, Inc., which is the assignee of record.

RELATED APPEALS AND INTERFERENCES

There are no related appeals, interferences, or judicial proceedings known to the Appellant which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

The present application under appeal has Claims 1 through 21. Claims 1 through 21 are rejected.

STATUS OF AMENDMENTS

No amendment was filed subsequent to final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1 recites a method of enabling a user to access a computer system 100 (e.g., Figure 6) and activating the computer system 100. The method includes capturing biometric data from the user desiring access to the computer system 100 having a user verification device 117 (e.g., Figure 6 and Figure 8) in response to initial interaction by the user with the user verification device 117, as depicted in Figure 11 and page 26, lines 1-21. Further, the method includes verifying the identity of the user using the biometric data, as depicted in Figure 11 and page 27, lines 1-8. Continuing, if verification of the identity of the user is successful, the computer system 100 is powered-up to a normal operation mode, as described in Figure 11 and page 27, lines 5-16. Also, the user is granted access to the computer system 100, as shown in Figure 11 and page 27, lines 5-20.

Independent Claim 12 recites a computer system 100 (e.g., Figure 6). The computer system 100 comprises a user verification device 117 (e.g., Figure 6) for capturing biometric data from a user, as described in Figure 6 and page 21, line 14 through page 22, line 2. The user initially interacts with the user verification device 117 to gain access to the computer system, as depicted in Figure 6 and page 22, lines 19-22. Moreover, the computer system 100 includes a memory device 104 (e.g., Figure 6) for storing a reference template representing stored biometric data from an authorized user, as described in Figure 10 and page 24, line 5 through page 25, line 12. Furthermore, the

computer system 100 includes a processor 101 (e.g., Figure 6) coupled to the user verification device 117 and to the memory device 104. The processor 101 is operative to receive the biometric data and to compare the biometric data with the reference template, as depicted in Figure 11 and page 27, lines 1-8. If a match is determined, the computer system 100 is powered-up from an inactive mode to a normal operation mode, as shown in Figure 11 and page 27, lines 5-16. Also, the user is granted access to the computer system, as shown in Figure 11 and page 27, lines 5-20.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether Claims 1, 3, 4-10, 12-19, and 21 are unpatentable under 35 U.S.C. 103 over Janiak et al. (Patent Application Publication No. US2002/0089410) in view of Maes et al. (U.S. Patent No. 6,016,476)?

Whether Claims 2, 11, and 20 are unpatentable under 35 U.S.C. 103 over Janiak et al. (Patent Application Publication No. US2002/0089410) in view of Maes et al. (U.S. Patent No. 6,016,476) and further in view of Haitani et al. (U.S. Patent No. 5,900,875)?

ARGUMENT

Rejections under 35 U.S.C. 103(a) over Janiak in view of Maes

Claims 1 and 3-10

Claims 1 and 3-10 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Janiak et al., U.S. Patent Application Publication No. 2002/0089410 (hereafter Janiak) in view of Maes et al., U.S. Patent No. 6,016,476 (hereafter Maes). Appellant respectfully submits that Claims 1 and 3-10 are patentable over Janiak in view of Maes for the reasons discussed below.

Independent Claim 1 recites:

> A method of enabling a user to access a computer system and activating said computer system, comprising the steps of:
> a) capturing biometric data from said user desiring access to said computer system having a user verification device in response to initial interaction by said user with said user verification device;
> b) verifying identity of said user using said biometric data; and
> c) ***if verification in said step b) is successful, powering-up said computer system to a normal operation mode and granting said user access to said computer system***. (emphasis added)

It is respectfully asserted that the combination of Janiak and Maes does not teach, suggest, or motivate all the limitations in Independent Claim 1. In particular, Independent Claim 1 recites the limitation, "***if verification in said step b) is successful, powering-up said computer system to a normal operation mode and granting said user access to said computer system*** " (emphasis added).

In contrast, Janiak discloses and shows in Figure 1 a biometric solution comprising a host device (14) and a removable fingerprint identification module or FIM (12), wherein the FIM (12) works with the host device (14) such that the occurrence of a biometric match or non-match will allow the host device (14) to perform custom specific functionalities. [Janiak; Figure 1; paragraph [0179]]. According to Janiak, the FIM (12) interconnects with the host device (14) to form a portable biometric reader, connects to the host device (14) so as not to interfere with normal operation of the host device (14), and may be removed from the host device (14) when desired. [Janiak; paragraph [0021]]. This implies that the host device (14) may be powered-up even if the FIM (12) has been removed and without capturing biometric data from the user to verify the user's identity. That is, the FIM (12) enables access control to functionality of the host device (14) after the host device (14) has been powered-up. Although the Examiner cites paragraphs 0025-0027 of Janiak as disclosing powering-up a device to a normal operation mode if the verification of the user's identity is successful, Janiak simply describes providing power to the FIM (12) components and fails to describe any relationship between powering-up the host device (14) and verification of the user's identity.

Further, while Janiak describes powering up the fingerprint sensor of the FIM (12) to obtain a fingerprint of a user, Janiak fails to disclose powering-up the host device (14) to a normal operation mode if verification of the user's identity by using the fingerprint (or biometric data) is successful, as in the invention of Independent Claim 1. In particular, Janiak only describes using the biometric

data to allow the host device (14) to perform custom specific functionalities and never describes the interaction between the powering on of the host device (14) and the FIM (12). Since the FIM (12) may be removed from the host device (14) when desired, this implies that the host device (14) is powered up without verification of the user's identity by using the user's fingerprint (or biometric data). [Janiak; Figure 1; paragraph [0021]].

Further, Maes is directed to utilizing biometric authorization to provide personal verification prior to processing user requested financial transactions and providing personal information. [Maes; Col. 1, lines 14-17]. In either the client/server mode or local mode, the PDA device (10) is fully powered, enabling the user to interact with the PDA device (10) before any biometric data is collected. [Maes; Col. 3, lines 38-67]. For the client/server mode, the user must periodically connect the powered PDA device (10) with a central server (60). [Maes; Col. 7, line 35 through Col. 8, line 27]. Once communication has been established, the user is prompted to enter certain verification data (e.g., biometric data). Id. For the local mode, the user selects a pre-enrolled credit card that is stored in memory (14) of the powered PDA device (10). [Maes; Col. 10, lines 29-65]. If the requested card information is found in memory (14), biometric verification must be performed before the card information can be written to the Universal Card (26). Id. In sum, the user is granted access to and interacts with the powered PDA device (10), wherein the user provides biometric data only when prompted by a specific transaction requested by the user. However, Maes does not teach, suggest, or motivate powering-up the computer system to a

normal operation mode and granting the user access to the computer system if verification of captured biometric data from the user is successful, as in the invention of Independent Claim 1. Therefore, it is respectfully submitted that Independent Claim 1 is patentable over the combination of Janiak and Maes and is in condition for allowance.

Dependent Claims 3-10 are dependent on allowable Independent Claim 1, which is allowable over the combination of Janiak and Maes. Hence, it is respectfully submitted that Dependent Claims 3-10 are patentable over the combination of Janiak and Maes for the reasons discussed above.

Claims 12-19 and 21

Claims 12-19 and 21 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Janiak et al., U.S. Patent Application Publication No. 2002/0089410 (hereafter Janiak) in view of Maes et al., U.S. Patent No. 6,016,476 (hereafter Maes). Appellant respectfully submits that Claims 12-19 and 21 are patentable over Janiak in view of Maes for the reasons discussed below.

Independent Claim 12 recites:

A computer system comprising:
a user verification device for capturing biometric data from a user, wherein said user initially interacts with said user verification device to gain access to said computer system;
a memory device for storing a reference template representing stored biometric data from an authorized user; and

a processor coupled to said user verification device and to said memory device, ***said processor operative to receive said biometric data and to compare said biometric data with said reference template, wherein if a match is determined, said computer system is powered-up from an inactive mode to a normal operation mode and said user is granted access to said computer system***. (emphasis added)

It is respectfully asserted that the combination of Janiak and Maes does not teach, suggest, or motivate all the limitations in Independent Claim 12. In particular, Independent Claim 12 recites the limitation, "***said processor operative to receive said biometric data and to compare said biometric data with said reference template, wherein if a match is determined, said computer system is powered-up from an inactive mode to a normal operation mode and said user is granted access to said computer system***," (emphasis added).

In contrast, Janiak discloses and shows in Figure 1 a biometric solution comprising a host device (14) and a removable fingerprint identification module or FIM (12), wherein the FIM (12) works with the host device (14) such that the occurrence of a biometric match or non-match will allow the host device (14) to perform custom specific functionalities. [Janiak; Figure 1; paragraph [0179]]. According to Janiak, the FIM (12) interconnects with the host device (14) to form a portable biometric reader, connects to the host device (14) so as not to interfere with normal operation of the host device (14), and may be removed from the host device (14) when desired. [Janiak; paragraph [0021]]. This implies that the host device (14) may be powered-up even if the FIM (12) has been

removed and without capturing biometric data from the user to verify the user's identity. That is, the FIM (12) enables access control to functionality of the host device (14) after the host device (14) has been powered-up. Although the Examiner cites paragraphs 0025-0027 of Janiak as disclosing powering-up a device to a normal operation mode if the verification of the user's identity is successful, Janiak simply describes providing power to the FIM (12) components and fails to describe any relationship between powering-up the host device (14) and verification of the user's identity.

Unlike the host device (14) of Janiak, the computer system of Independent Claim 12 is powered-up from an inactive mode to a normal operation mode and the user is granted access to the computer system if the biometric date from an authorized user matches the captured biometric data from a user desiring to access the computer system. That is, there is a dependent relationship between powering-up the computer system to a normal operation mode and verification of the user's identity. The computer system powers up to the normal operation mode after successfully matching the biometric data of the user desiring access with the biometric data of an authorized user.

Further, Maes is directed to utilizing biometric authorization to provide personal verification prior to processing user requested financial transactions and providing personal information. [Maes; Col. 1, lines 14-17]. In either the client/server mode or local mode, the PDA device (10) is fully powered, enabling

the user to interact with the PDA device (10) before any biometric data is collected. [Maes; Col. 3, lines 38-67]. For the client/server mode, the user must periodically connect the powered PDA device (10) with a central server (60). [Maes; Col. 7, line 35 through Col. 8, line 27]. Once communication has been established, the user is prompted to enter certain verification data (e.g., biometric data). Id. For the local mode, the user selects a pre-enrolled credit card that is stored in memory (14) of the powered PDA device (10). [Maes; Col. 10, lines 29-65]. If the requested card information is found in memory (14), biometric verification must be performed before the card information can be written to the Universal Card (26). Id. In sum, the user is granted access to and interacts with the powered PDA device (10), wherein the user provides biometric data only when prompted by a specific transaction requested by the user. However, Maes does not teach, suggest, or motivate powering-up the computer system to a normal operation mode and granting the user access to the computer system if the biometric date from an authorized user matches the captured biometric data from a user desiring to access the computer system, as in the invention of Independent Claim 12. Therefore, it is respectfully submitted that Independent Claim 12 is patentable over the combination of Janiak and Maes and is in condition for allowance.

Dependent Claims 13-19 and 21 are dependent on allowable Independent Claim 12, which is allowable over the combination of Janiak and Maes. Hence, it is respectfully submitted that Dependent Claims 13-19 and 21 are patentable over the combination of Janiak and Maes for the reasons discussed above.

Rejections under 35 U.S.C. 103(a) over Janiak in view of Maes and Haitani

Claims 2 and 11

Claims 2 and 11 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Janiak et al., U.S. Patent Application Publication No. 2002/0089410 (hereafter Janiak), in view of Maes et al., U.S. Patent No. 6,016,476 (hereafter Maes), and further in view of Haitani et al., U.S. Patent No. 5,900,875 (hereafter Haitani). Appellant respectfully submits that Claims 2 and 11 are patentable over Janiak in view of Maes and Haitani for the reasons discussed below.

Dependent Claims 2 and 11 are dependent on allowable Independent Claim 1, which is allowable over the combination of Janiak and Maes. Moreover, Haitani does not teach, suggest, or motivate capturing biometric data from the user desiring access to the computer system having a user verification device in response to initial interaction by the user with the user verification device, as in the invention of Independent Claim 1. Further, Haitani does not teach, suggest, or motivate verifying identity of the user using the biometric data, as in the invention of Independent Claim 1. Also, Haitani does not teach, suggest, or motivate if verification of user's identity is successful, powering-up the computer system to a normal operation mode and granting the user access to the computer system, as in the invention of Independent Claim 1. Therefore Independent Claim 1 is patentable over the combination of Janiak, Maes, and Haitani. Since Dependent Claims 2 and 11 depend from Independent Claim 1, it

is respectfully submitted that Dependent Claims 2 and 11 are patentable over the combination of Janiak, Maes, and Haitani for the reasons discussed above.

Claim 20

Claim 20 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Janiak et al., U.S. Patent Application Publication No. 2002/0089410 (hereafter Janiak), in view of Maes et al., U.S. Patent No. 6,016,476 (hereafter Maes), and further in view of Haitani et al., U.S. Patent No. 5,900,875 (hereafter Haitani). Appellant respectfully submits that Claim 20 is patentable over Janiak in view of Maes and Haitani for the reasons discussed below.

Dependent Claim 20 is dependent on allowable Independent Claim 12, which is allowable over the combination of Janiak and Maes. Moreover, Haitani does not teach, suggest, or motivate a user verification device for capturing biometric data from a user, wherein the user initially interacts with the user verification device to gain access to the computer system, as in the invention of Independent Claim 12. Further, Haitani does not teach, suggest, or motivate a memory device for storing a reference template representing stored biometric data from an authorized user, as in the invention of Independent Claim 12. Also, Haitani does not teach, suggest, or motivate a processor coupled to the user verification device and to the memory device, the processor operative to receive the biometric data and to compare the biometric data with the reference template, wherein if a match is determined, the computer system is powered-up

from an inactive mode to a normal operation mode and the user is granted access to the computer system, as in the invention of Independent Claim 12. Therefore Independent Claim 12 is patentable over the combination of Janiak, Maes, and Haitani. Since Dependent Claim 20 depends from Independent Claim 12, it is respectfully submitted that Dependent Claim 20 is patentable over the combination of Janiak, Maes, and Haitani for the reasons discussed above.

For the extensive reasons advanced above, Appellant respectfully but forcefully contends that each claim (Claims 1-21) is patentable. Therefore, reversal of all rejections is courteously solicited.

Respectfully submitted,

WAGNER, MURABITO & HAO, LLP

Dated: 5/5/2006

Jose S. Garcia

Jose S. Garcia
Registration No. 43,628

Two North Market Street, Third Floor
San Jose, CA 95113
(408) 938-9060

CLAIMS APPENDIX

1. A method of enabling a user to access a computer system and activating said computer system, comprising the steps of:

a) capturing biometric data from said user desiring access to said computer system having a user verification device in response to initial interaction by said user with said user verification device;

b) verifying identity of said user using said biometric data; and

c) if verification in said step b) is successful, powering-up said computer system to a normal operation mode and granting said user access to said computer system.

2. A method as recited in Claim 1 wherein said step a) comprises:

generating an interrupt to alert said computer system that said user desires access to said computer system.

3. A method as recited in Claim 1 wherein said step b) comprises:

comparing said biometric data with a reference template representing stored biometric data of an authorized user.

4. A method as recited in Claim 1 further comprising the step of:

automatically invoking an application program upon entering said normal operation mode.

5. A method as recited in Claim 1 further comprising the steps of:

capturing new biometric data from said user using said user verification device during said normal operation mode according to a programmable schedule; and

verifying identity of said user using said new biometric data to continue access by said user.

6. A method as recited in Claim 1 wherein said biometric data is one of a thumbprint, a fingerprint, a magnetic characteristic, a color characteristic, a temperature characteristic, a geometric characteristic, and a combination thereof of said user.

7. A method as recited in Claim 1 wherein said user verification device comprises a biometric sensor.

8. A method as recited in Claim 1 wherein said user initiates said step a) by pressing said user verification device.

9. A method as recited in Claim 1 wherein said user initiates said step a) by swiping said user verification device.

10. A method as recited in Claim 1 wherein said user initiates said step a) by touching said user verification device.

11. A method as recited in Claim 1 wherein said user verification device has a button-shape.

12. A computer system comprising:

a user verification device for capturing biometric data from a user, wherein said user initially interacts with said user verification device to gain access to said computer system;

a memory device for storing a reference template representing stored biometric data from an authorized user; and

a processor coupled to said user verification device and to said memory device, said processor operative to receive said biometric data and to compare said biometric data with said reference template, wherein if a match is determined, said computer system is powered-up from an inactive mode to a normal operation mode and said user is granted access to said computer system.

13. A computer system as recited in Claim 12 wherein an application program stored in said memory device is automatically invoked upon entering said normal operation mode.

14. A computer system as recited in Claim 12 wherein said user is prompted to interact with said user verification device during said normal operation mode according to a programmable schedule so that new biometric

data can be captured by said user verification device and processed by said processor to continue access by said user.

15. A computer system as recited in Claim 12 wherein said biometric data is one of a thumbprint, a fingerprint, a magnetic characteristic, a color characteristic, a temperature characteristic, a geometric characteristic, and a combination thereof of said user.

16. A computer system as recited in Claim 12 wherein said user verification device comprises a biometric sensor.

17. A computer system as recited in Claim 12 wherein said user interacts with said user verification device by pressing said user verification device.

18. A computer system as recited in Claim 12 wherein said user interacts with said user verification device by swiping said user verification device.

19. A computer system as recited in Claim 12 wherein said user interacts with said user verification device by touching said user verification device.

20. A computer system as recited in Claim 12 wherein said user verification device has a button-shape.

21. A computer system as recited in Claim 12 wherein said computer system comprises a personal digital assistant.

EVIDENCE APPENDIX

No evidence is relied upon by the Appellant in the appeal.

RELATED PROCEEDINGS APPENDIX

None